

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**



AIR FORCE INSTRUCTION 33-101

18 NOVEMBER 2008

Incorporating Change 1, 21 JULY 2011

**ELLSWORTH AIR FORCE BASE
Supplement**

17 OCTOBER 2012

Communications and Information

**COMMANDERS GUIDANCE AND
RESPONSIBILITIES**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-publishing.af.mil/.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6PP

Certified by: SAF/XCP-2
(Brig Gen Ronnie Hawkins)

Pages: 33

Supersedes: AFI 33-101, 24 July 1998

(ELLSWORTHAFB)

OPR: 28 CS/SCOS

Certified by: 28 CS/CC
(Major Robert H. Kelly)

Pages: 6

This Instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*, and is consistent with the policy in AFPD 33-2, *Information Assurance (IA) Program*. It identifies commanders' responsibilities for supporting the management of the Air Force-provisioned portion of the Global Information Grid (AF-GIG) Enterprise Information Environment (EIE)/IT Infrastructure mission area to meet mission readiness and warfighting capabilities. It provides management procedures for commanders to ensure availability, interoperability, and maintainability of communications and information systems in support of mission readiness and warfighting capability. This Instruction covers general guidance and responsibilities for effective and efficient management of systems throughout their life-cycle. This Instruction applies to all commanders and identifies a commander's responsibilities for effective and efficient Information Resource Management (IRM). This Instruction applies to all

Air Force military, civilians, and contractor personnel under contract by the Department of Defense (DoD). This Instruction applies to the Air National Guard (ANG) and the Air Force Reserve Component (AFRC). Direct questions or comments on the contents of this Instruction, through appropriate command channels, to the Air Force Chief, Warfighting Integration and Chief Information Officer, Policy and Compliance Division, (SAF/A6PP), 1800 Air Force Pentagon, Washington DC 20330-1800. Send recommended changes and conflicts between this and other publications, using Air Force (AF) Form 847, *Recommendation for Change of Publication*, to SAF/A6PP. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>. See Attachment 1 for a glossary of references and supporting information.

(ELLSWORTHAFB) AFI 33-101, dated 18 November 2008, is supplemented as follows:

This instruction implements **Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems***, and is used in conjunction with AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation and Non-appropriated Fund Instrumentalities*; and Air Force Manual (AFMAN) 23-110, *United States Air Force Supply Manual*. It establishes responsibilities and outlines procedures for obtaining public address (PA) system support. The purpose of this instruction is to provide guidance to Ellsworth Air Force Base (EAFB) personnel on the capabilities and limitations of PA support provided by the 28th Communications Squadron (28 CS). This instruction also provides information on alternate means of obtaining support. This instruction applies to all units on EAFB, except for the United States Air Force Reserve and Air National Guard units and members. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS)

(ELLSWORTHAFB) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>. Send comments and suggested changes to this supplement through channels, using AF Form 847, *Recommendation for Change of Publication*, to 28 CS/SCOK, 1000 Ellsworth St. Rushmore Center, Ellsworth AFB, SD 57706.

SUMMARY OF CHANGES

This change incorporates interim change (IC) 1 and defines commanders' roles and responsibilities related to the management and sustainment of the cyberspace infrastructure. Major changes for roles and responsibilities are included for installation commanders, MAJCOM Communications and Information Systems Officers (CSOs) and information staff elements, and installation CSOs. Effective documentation and management of the cyberspace infrastructure is essential in ensuring the continuous security, operational availability, and reliability of systems and equipment supporting the Air Force mission. These changes are effective immediately. A margin bar indicates newly revised material.

(ELLSWORTHAFB) This revision is a complete rewrite. This supplement incorporates new information from the original AFI that was updated on 18 November 2008. The revision

explains which functions are supported, updated the Point of Contact (POC) in the Communications Squadron for local users, explains the customers responsibilities for services, the Communications Squadron responsibilities and outlines the request process for Public Address (PA) support. Added attachment 4.

1.	Introduction.	3
2.	Applicability.	3
3.	Responsibilities.	4
4.	Information Assurance Programs.	5
5.	IT Management Programs.	7
6.	Information Management Programs.	10
7.	Information Collection, Records, and Forms	13
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		14
Attachment 1—(ELLSWORTHAFB) GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		23
Attachment 2—COMMUNICATIONS AND INFORMATION SYSTEMS OFFICER DUTIES		25
Attachment 3—DELETED		29
Attachment 4—(Added-ELLSWORTHAFB) PUBLIC ADDRESS (PA) RESPONSIBILITIES AND PROCEDURES		30

1. Introduction.

1.1. In an effort to meet the growing needs of today's warfighter, great strides are being made to improve the capabilities offered by the Air Force provisioned portion of the Global Information Grid (GIG). Today's warfighters are increasingly using these capabilities and have responsibilities for ensuring effective and efficient use and management of this resource. This increased reliance on warfighters is a result of the mainstreaming of technology and its integration into almost all activities of warfighting and support operations. This AFI identifies a commander's responsibilities for ensuring effective and efficient management of Information Technology (IT), Information Management (IM), and Information Assurance (IA). Compliance ensures appropriate personnel are assigned/appointed to accomplish identified duties.

2. Applicability.

2.1. This instruction applies to all commanders and identifies a commander's responsibilities for effective and efficient management of IT, Information management (IM), and IA. This does not apply to systems under the purview of the Director of National Intelligence (DNI) and Intelligence agencies.

3. Responsibilities.

3.1. Commanders or equivalent at all levels will maintain these responsibilities through the following programs:

3.1.1. Assign an organizational Information Assurance Officer (IAO) to execute IA responsibilities protecting and defending information systems by ensuring the availability, integrity, confidentiality, authentication, and non-repudiation of data through the application of IA measures outlined in [paragraph 4](#). Additional (subordinate) IAO positions may be assigned for additional support at the discretion of organizations or based upon mission requirements; however, only one primary and one alternate IAO is required. Execute IAO responsibilities for the following programs:

- 3.1.1.1. Network and Computer Security Program as stated in [paragraph 4.1](#).
- 3.1.1.2. Communications Security (COMSEC) Program as stated in [paragraph 4.2](#).
- 3.1.1.3. Emissions Security (EMSEC) Program as stated in [paragraph 4.3](#).
- 3.1.1.4. Identity Management Program as stated in [paragraph 4.4](#).
- 3.1.1.5. IA Notice and Consent certification program as stated in [paragraph 4.5](#).

3.1.2. Execute management responsibilities to improve the efficiency and effectiveness of Air Force activities and delivery of services through the proper employment of:

- 3.1.2.1. Mobile Satellite Services Program as stated in [paragraph 5.1](#).
- 3.1.2.2. Frequency Management Program as stated in [paragraph 5.2](#).
- 3.1.2.3. IT Asset Management Program as stated in [paragraph 5.3](#).
- 3.1.2.4. Software Management Program as stated in [paragraph 5.4](#).
- 3.1.2.5. Voice Services Program as stated in [paragraph 5.5](#).
- 3.1.2.6. Messaging Services Program as stated in [paragraph 5.6](#).

3.1.3. Execute IM responsibilities for management and control of all Air Force information resources under their purview as outlined in the:

- 3.1.3.1. Records Management Program as stated in [paragraph 6.1](#).
- 3.1.3.2. Information Collection and Reports Management Program as stated in [paragraph 6.2](#).
- 3.1.3.3. Privacy Act Program as stated in [paragraph 6.3](#).
- 3.1.3.4. Section 508 of the Rehabilitation Act Compliance Program as stated in [paragraph 6.4](#).
- 3.1.3.5. Base Locator Services as stated in [paragraph 6.5](#).
- 3.1.3.6. Official Mail Program as stated in [paragraph 6.6](#).
- 3.1.3.7. Freedom of Information Act (FOIA) Program as stated in [paragraph 6.7](#).
- 3.1.3.8. Web management as stated in [paragraph 6.8](#).

3.2. Major Commands (MAJCOMs) will:

3.2.1. Execute duties described in [paragraph 3.1](#).

3.2.2. Designate in writing a Communications Systems Officer (CSO) and a single staff element for overall management of communications and information systems. The CSO provides technical advice to the commander (see [Attachment 2](#) for detailed responsibilities).

3.2.3. Establish a MAJCOM IA Office to implement and oversee the MAJCOM IA Program, as stated in [paragraph 3](#).

3.3. Installation Commander or equivalent will:

3.3.1. Execute duties described in [paragraph 3.1](#).

3.3.2. Designate in writing the installation/host wing communications officer as the installation CSO. The installation CSO is responsible for meeting the communications and information mission needs of the entire installation, assigned tenant units, and geographically separated units (GSUs) not receiving support from another host wing, command, or Service (see [Attachment 2](#)).

3.3.3. Ensure CSO establishes a periodic (annually, at a minimum) wing-level planning forum to endorse the base blueprint in the Cyberspace Infrastructure Planning System (CIPS). Reference Methods and Procedures Technical Order (MPTO) 00-33D-3003, *Managing the Cyberspace Infrastructure with the Cyberspace Infrastructure Planning System*.

3.3.4. Establish a Wing IA Office to implement and oversee the installation's IA Program, as stated in [paragraph 3](#). The Wing IA office addresses all IA requirements on the installation, including those of tenant units (i.e., FOAs, DRUs, and other MAJCOM units) unless formal agreements indicates otherwise.

3.4. Unit Commanders or Tenant Units will:

3.4.1. Execute duties described in [paragraph 3.1](#).

3.4.2. Appoint in writing a tenant CSO to serve as their single focal point and accountable officer for the communications and information systems of their respective activities. Define specific tenant and installation CSO responsibilities in the support agreement or similar document.

3.4.3. Coordinate with the installation CSO to ensure their systems will integrate and interoperate, when necessary, with the GIG, AF-GIG or host base systems.

4. Information Assurance Programs. Supports the principles of availability, integrity, confidentiality, authentication, and non-repudiation of information and information systems for the purpose of protecting and defending the operation and management of Air Force IT and National Security System (NSS) assets and operations.

4.1. Network and Computer Security (COMPUSEC) Program. Ensures Air Force information systems operate effectively by protecting and maintaining the confidentiality, integrity and availability of information system resources and information processed

throughout the system's life cycle. For additional program information, reference AFI 33-200, *Information Assurance (IA) Management*.

4.1.1. Establish a MAJCOM IA Office to implement and oversee the MAJCOM Computer Security (COMPUSEC) Program.

4.1.2. Installation Wings will establish COMPUSEC in the Wing IA Office

4.1.3. Unit Commanders shall designate the organizational Information Assurance Officer (IAO) as the individual(s) responsible for COMPUSEC matters in the organization.

4.2. Communications Security (COMSEC) Program. The Air Force COMSEC program meets Public Law, national, and DoD requirements to secure or protect classified and sensitive information processed using Air Force information systems. For additional program information reference AFI 33-201, Volume 1, *Communications Security (COMSEC)* (will become part of AFI 33-200).

4.2.1. Establish the MAJCOM COMSEC program in the MAJCOM IA Office to implement and oversee MAJCOM COMSEC.

4.2.2. Installation Commanders will:

4.2.2.1. Manage the overall COMSEC posture of their installation through the Wing IA Office.

4.2.2.2. Appoint in writing one primary and at least one alternate COMSEC manager to oversee the wing COMSEC program. The Wing commander may delegate appointment authority to the unit commander of the supporting COMSEC account.

4.2.3. Supported Unit Commanders will:

4.2.3.1. Appoint in writing sufficient COMSEC Responsible Officers (CROs) or Secure Voice Responsible Officers (SVROs) and alternates to support their unit's COMSEC mission. Do not appoint a SVRO where there is a CRO unless CRO workload otherwise dictates.

4.2.3.2. Appoint in writing an investigating officer who determines results and recommends corrective actions for COMSEC deviations. Review incident reports and provide summary comments.

4.2.3.3. Unit commanders with COMSEC Maintenance Technicians will appoint in writing a COMSEC Equipment Certifier who certifies the DD Form 1435, *COMSEC Maintenance Training and Experience Record*, or automated product for certification of technicians following guidance in AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*.

4.3. Emission Security (EMSEC) Program. The objective of EMSEC is to contain compromising emanations within an inspectable space in order to deny access to classified and, in some instances, unclassified information. For additional program information reference AFI 33-200 and AFSSI 7700, *Emission Security*.

4.3.1. MAJCOMs will establish an EMSEC program within the MAJCOM IA office.

4.3.2. Installation Wing will establish an EMSEC program in the host wing IA office.

4.3.3. Unit commanders designate the organizational IAO as the EMSEC representative to identify and work unit issues with host installation EMSEC representatives.

4.4. Identity Management Program. The Air Force Identity Management program encompasses a set of capabilities including Public Key Infrastructure (PKI), Common Access Cards (CACs), and Air Force Directory Services (AFDS). For additional PKI program information reference AFI 33-200.

4.4.1. MAJCOMs will:

4.4.1.1. Ensure all eligible personnel receive their DoD PKI certificates on the CAC and use them to authenticate to the NIPRNET and public-key enabled websites and applications.

4.4.1.2. Establish a network of Local Registration Authorities (LRA) and Trusted Agents (TA) to support NIPRNET and SIPRNET software certificate requirements. These resources will provide user registration and certificate management support to include support to deployed, mobile, contingency, tactical, and AF supported COCOM users. LRAs and TAs will also provide device certificates on unclassified and classified networks and other than CAC-based certificate support on the NIPRNET.

4.4.1.3. Identify personnel to perform LRA and TA duties as required and coordinate with the AF PKI SPO for LRA training and specific guidance. Ensure LRAs and TAs are complying with the AF LRA Certificate Practice Statements and DoD X.509 Certificate Policy.

4.5. IA Notice and Consent Program. The Notice and Consent process ensures authorized users are provided with legally-sufficient notice that their use of these systems constitutes consent to monitoring for authorized purposes. For additional information about the process reference AFI 33-219, *Telecommunication Monitoring and Assessment Program* (will become part of AFI 33-200).

4.5.1. Commanders at all levels will:

4.5.1.1. Provide legally-sufficient notice to users stating all DoD telecommunications systems and information systems are subject to monitoring for authorized purposes and the use of these systems constitutes consent to monitoring.

4.5.1.2. Designate the organizational IAO as individual(s) responsible for ensuring compliance with the notice and consent requirements.

5. IT Management Programs. Established to ensure appropriate and effective use of IT resources, ensure their availability, and improve the efficiency and effectiveness of the Air Force consistent with IT commodity council policy and vision.

5.1. Mobile Satellite Services (MSS) Program. Provides the framework for acquiring, managing, and reporting the use of Mobile Satellite Services. For additional program information, reference AFI 33-134, *Mobile Satellite Services Management*.

5.1.1. MAJCOMs will:

5.1.1.1. Appoint in writing a MAJCOM Mobile Satellite Services (MSS) manager.

5.1.1.2. Send name, rank, Defense Switched Network (DSN) number, and e-mail address to Air Force MSS Lead Command, HQ AFCA/ES, within 15 days of appointment.

5.1.2. Supported units will appoint, in writing, a primary and alternate unit MSS manager.

5.2. Electromagnetic Spectrum Management Program. Sets the policy for managing electromagnetic spectrum supporting the Air Force mission. For additional program information, reference AFI 33-118, *Electromagnetic Spectrum Management* and AFMAN 33-120, *Electromagnetic Spectrum Management*.

5.2.1. MAJCOMs will maintain electromagnetic spectrum management function in accordance with AFI 33-118.

5.2.2. Installation Commanders are responsible for all electromagnetic radiation emanating from the installation and from those outlying activities hosted by the installation. Installation Commanders ensure a viable Radio Frequency (RF) management program is in place and supports installation requirements. The installation commander will prohibit any on-installation RF emitter from operating (cease and desist) when anticipating or resolving interference to mission essential electromagnetic equipment. Resolve interference IAW AFI 10-707, *Spectrum Interference Resolution Program*.

5.3. IT Asset Management (ITAM) Program. Identifies responsibilities for supporting AF IT equipment. For additional program information, reference AFI 33-112, *Information Technology Hardware Asset Management*.

5.3.1. MAJCOMs will:

5.3.1.1. Appoint in writing a MAJCOM Equipment Control Officer (MECO) to oversee and implement the IT Asset Management Program for the Command unless under HQ AFCA consolidated MECO construct as described in AFI 33-112, *Information Technology Hardware Asset Management*.

5.3.1.2. Review their MAJCOM-unique systems at least once every three years to ensure the continued need for the system.

5.3.1.2.1. Review system requirements and involve the MAJCOM IA office in review of any application interfacing with NIPRNET or SIPRNET.

5.3.1.2.2. Determine if the operation and maintenance costs warrant continued operation.

5.3.2. Unit Commanders or equivalent will:

5.3.2.1. Appoint in writing primary and alternate Equipment Custodian(s) (ECs) IAW AFI 33-112.

5.3.2.2. Provide guidance and procedures to ensure adequate protection and oversight is afforded to IT and National Security System (NSS) assets under their control. As the responsible officer, commanders are charged with custody, care, and safekeeping over all IT and NSS assets within their organization.

5.3.2.3. Budget for maintenance of computer systems that are not the responsibility of the installation CSO.

5.4. Software Management Program. Identifies the responsibilities associated with planning, developing, using, maintaining, or supporting computer software to effectively and efficiently complete assigned missions. It applies to Air Force-procured COTS software and software developed for unique Air Force purposes (other than software internal to a weapon system; see AFPD 63-1, *Capability-Based Acquisition System*). For additional program information, reference AFI 33-114, *Software Management*.

5.4.1. All MAJCOM/DRU/FOA CSOs will:

5.4.1.1. Conduct and document an annual inventory of software licenses as required by Executive Order (EO) 13103, Computer Software Piracy.

5.4.1.2. Establish a process to track their unique software licenses.

5.4.1.3. Develop performance measurements and metrics for software license requirements as required by EO 13103.

5.4.2. Installation and Unit Commanders or equivalent will:

5.4.2.1. Contact the responsible functional or program management office before purchasing software licenses to determine if COTS software licenses are available, or if there is a standard product to buy. Reference path on AF portal: Air Force\Enterprise IT Initiatives\Enterprise COTS Software Agreements.

5.4.2.2. Coordinate with the Air Force Materiel Command (AFMC) designated product center to obtain volume pricing for products available through the DoD Enterprise Software Initiative (ESI). The Defense Federal Acquisition Regulation (DFAR) Supplement, Part 208, Required Sources of Supplies and Service, Subpart 208.74, Enterprise Software Agreements (ESA), requires purchasers to first consider DoD Enterprise Software Agreements found at <https://www.esi.mil>.

5.4.2.3. Coordinate with the installation CSO or servicing Network Control Center (NCC) before acquiring, developing, or implementing any software and comply with all IA program requirements in accordance with AFI 33-200.

5.4.2.4. Prepare annual inventories of the software present on its computers in accordance with AFI 33-114.

5.5. Voice Services Program. Identifies the policy and responsibilities associated with planning, developing, using, maintaining, or supporting voice services to effectively and efficiently complete assigned missions. For additional program information, reference AFI 33-111, *Voice Systems Management*.

5.5.1. Installation Commanders will establish local guidance for handling incoming official collect telephone calls.

5.5.2. When the host base does not require flat rate long distance telephone service, such a service is a special requirement and the base tenant organization must pay for it.

5.5.3. Unit Commanders and Tenant Units will:

5.5.3.1. Appoint in writing Primary and Alternate Telephone Control Officers (TCO) to the installation CSO. The unit's TCO is the individual who authorizes and controls long distance toll calls, DSN access authorization, and acts as the focal point for reviewing all unit communications requirements and requests for service before submitting them to the communications squadron.

5.5.3.2. Tenant units shall not procure commercial voice services and equipment without approval of the host installation CSO. Exceptions to this guidance must be clearly documented in the Host Tenant Support Agreement or similar document.

5.6. Messaging Services Program. Provides procedures and assigns responsibilities for establishing and managing MAJCOM Message Service Centers (MMSC). For additional program information, reference AFI 33-113, *Managing Air Force Messaging Centers*.

5.6.1. Installation Commanders will:

5.6.1.1. Appoint in writing sub-registration authority and mail list/address list cognizant authorities for message services as needed.

5.6.1.2. Ensure local control center and base distribution point accounts are established.

5.6.1.3. Appoint in writing a Base Distribution Point account manager.

5.6.2. Unit Commanders and Tenant Units will:

5.6.2.1. Establish an alternate delivery point for Urgent (High Precedence) messages when organizational accounts are not manned on a 24-hour, 7-day a week basis (24/7).

5.6.2.2. Provide an after-hours notification personnel listing to the alternate delivery POC.

5.6.2.3. Designate release authority, as necessary.

6. Information Management Programs. Establish policy and responsibilities for the representation of, access to, and maintenance, management, analysis, distribution, and integration of "information assets" (all forms of data and content) across Air Force information sources. Ensures the ability to discover, access, store, protect, share, and exploit mission-critical information regardless of its physical location, media, source, owner, or other defining characteristics.

6.1. Records Management Program. Establishes policy and assigns responsibilities for life-cycle management (e.g., creation, maintenance, use, and disposition) of information as records in all media through the Air Force Records Management Program. The Air Force requires an organized network of Record Managers (RM) at MAJCOMs, DRUs, FOAs, and installations for managing the program and ensuring compliance at all levels. For additional program information reference AFI 33-322, *Records Management Program*.

6.1.1. MAJCOM (Commander or senior communications and information official) will appoint a Command Records Manager (CRM). Upon appointment or subsequent change of CRM, notify SAF/XCPP of the name, grade or rank, telephone number, office symbol, and organizational electronic mail address of the appointee.

6.1.2. DRU (commander or senior communications and information official) will appoint a Records Manager (RM). CRM responsibility applies to Air Force DRUs and Air National Guard for the purposes of executing the Air Force Records Management Program. **NOTE:** CRM responsibilities are performed by the 11th Wing for offices of record in the Secretariat, HQ USAF, and at Bolling AFB DC.

6.1.3. FOA Commanders or senior communications and information official must appoint an Agency Records Manager (ARM).

6.1.4. Installation Commanders or senior communications and information official will appoint an installation RM and notify the appropriate CRM, providing the same information as in [paragraph 5.1.1](#). At levels below MAJCOM, where there is a communications squadron, the RM is the Chief of the Office of Records (COR) function.

6.1.5. Unit commanders will appoint one or more Functional Area Records Managers (FARM). One or more FARMS may be required based on the span of control, the complexities of the mission, and the size of the organization's functional areas. Additionally, they will ensure COR responsibilities are assigned.

6.1.6. Unit commanders will work with their Wing/Unit RM as necessary to support the program.

6.2. Information Collection and Reports Management Program. Establishes procedures for information collecting and reporting of internal, public, and interagency requirements. For additional program information, reference AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will become part of AFI 33-394, *Knowledge, Information and Data Management*).

6.2.1. Each HQ USAF and SAF functional organization, MAJCOM, DRU, and FOA will appoint in writing an Information Collections and Reports (ICR) Manager and send the Air Force Information Management Control Officer (SAF/XCPP) the name, functional address symbol, e-mail address, and telephone number when a new ICR Manager is assigned.

6.3. Privacy Act Program. Implements the Privacy Act of 1974 and applies to records on living US citizens and permanent resident aliens that are retrieved by name or personal identifier. The program provides guidance on collecting and disseminating personal information in general. For additional program information reference AFI 33-332, *Privacy Act Program*.

6.3.1. MAJCOM, FOA, and DRU commanders will appoint in writing a command Privacy Act officer, and send the name, office symbol, phone number, and e-mail address to SAF/XCPP.

6.3.1.1. Command Privacy Act Officers may authorize appointment of unit Privacy Act monitors to assist with implementation of the program.

6.3.2. Installation Commanders appoint installation Privacy Act Officers in writing to the command Privacy Act Officer NLT 60 days prior to incumbent installation Privacy Act Officer's date of departure/separation, to allow time for proper training and turnover.

6.4. Section 508 of the Rehabilitation Act Compliance Program. Establishes the Air Force corporate approach to Section 508 implementation and follows the guidelines established by the Office of the Secretary of Defense (OSD) of “centralized management with decentralized execution.” This approach provides a corporate strategy addressing all legal requirements and provides maximum access to Electronic and Information Technology (E&IT) while maintaining full mission focus and capabilities and giving people with disabilities the opportunity to maximize their contribution to the success of the Air Force mission. For additional program information, reference AFI 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities, Section 508*.

6.4.1. MAJCOM, FOA, and DRU commanders will identify a unit to support the Section 508 Program and provide Section 508 training for personnel within their units who are involved in the Section 508 process.

6.4.2. Installation Level Section 508 support organizations will execute Section 508 compliance guidance distributed by the Section 508 Management Office and posted at https://www.cio.hq.af.mil/private/private_section_508.shtml.

6.5. Base Locator Services. Installation and organization personnel locator services are defined in AFI 33-329, *Base and Unit Personnel Locators*.

6.5.1. Installation commanders will determine if their base will provide locator services and, if provided, the scope of service (none, limited, or full), category of release (official, personal, or both), and hours of availability. Commanders determine whether to add civilian and/or contractor personnel to the base locator, select the designated base locator service provider, and establish procedures for base locator use.

6.5.2. Unit commanders will decide if a personnel locator is required for their units and if so, consider whether the base locator meets the locator requirement. If a separate unit locator is required, organizational commanders determine the scope of service, category of release, and hours of availability. Commanders determine whether to include civilian and/or contractor personnel in the unit locator and who provides unit locator services. They also establish procedures for unit locator use.

6.6. Official Mail Program. Establishes postal and official mail/distribution operational guidance and policy across the enterprise to ensure the Air Force can support in-garrison and Aerospace Expeditionary Force requirements. Prescribes how the Air Force operates the Military Postal Service (MPS) as an extension of the US Postal Service, consistent with public law and federal regulations. For additional program information reference DoDM 4525.8/AFMAN 33-306, *DOD Official Mail Manual*.

6.6.1. Commanders, staff agency chiefs, deputies, executive officers, or Activity Distribution Office (ADO) directors will appoint assigned individuals to receive and dispatch communications as directed in DoDM 4525.8/AFMAN 33-306, *DOD Official Mail Manual*. The appointing official is responsible to ensure security clearances are verified by the applicable security manager.

6.6.2. Installation commanders must provide facilities, equipment, vehicles, resources, and services for efficient Official Mail Center operation.

6.7. Freedom of Information Act (FOIA) Program. Prescribes how the Air Force makes information on operation and activities publicly available in accordance with DODD 5400.7, *DoD Freedom of Information Act Program* requirements. For additional program information, reference DoD 5400.7- R/Air Force Supplement, *DoD Freedom Of Information Act Program*.

6.7.1. Installation commanders will establish a FOIA electronic reading room in accordance with DoD 5400.7-R AFSUP.

6.7.2. MAJCOM, FOA, and DRU commanders will support this program by appointing a FOIA manager in writing and implementing the instructions contained DoD 5400.7-R AFSUP.

6.8. Web Management. Provides policy and procedural guidance with respect to establishing, operating, and maintaining web sites in the Air Force. For additional program information reference AFI 33-129, *Web Management And Internet Use*.

6.8.1. Commanders at all levels are responsible for the content of the information posted on their public and private web pages/sites. Commanders will:

6.8.1.1. Initiate and sign/approve appointment letters for their web server administrators, web masters, and web page maintainers.

6.8.1.2. Ensure their web server administrators, web masters, web page maintainers, and information providers receive training in accordance with AFI 33-129, *Web Management and Internet Use*.

7. Information Collection, Records, and Forms

7.1. Information Collections. No information collections are accomplished by this publication.

7.2. Records. The program records created as a result of the processes prescribed in this publication are maintained in accordance with AFMAN 33-363 and disposed of in accordance with the AFRIMS RDS located at <https://www.my.af.mil/gcss-af61a/afirms/afirms/>.

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

(ELLSWORTHAFB)

JEFFREY B. TALIAFERRO, Colonel, USAF
Commander, 28th Bomb Wing

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Executive Order 13103, *Computer Software Piracy*, September 30, 1998

DFAR Supplement, Part 208, *Required Sources of Supplies and Service*, Subpart 208.74, *Enterprise Software Agreements (ESA)*, Revised October 26, 2006

DoDM 4525.8_AFMAN 33-306, *DoD Official Mail Manual*, 21 October 2006

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994

AFPD 33-1, *Information Resources Management*, 27 June 2006

AFI 10-707, *Spectrum Interference Resolution Program*, 20 June 2005

AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*, 22 March 2001

AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*, 1 October 2000

AFI 32-7062, *Air Force Comprehensive Planning*, 1 October 1997, Certified Current 13 November 2009

AFI 33-111, *Voice Systems Management*, 24 March 2005, through Change 2, 11 July 2006

AFI 33-112, *Information Technology Hardware Asset Management*, 20 April 2006

AFI 33-113, *Managing Air Force Messaging Centers*, 6 February 2007

AFI 33-114, *Software Management*, 13 May 2004

AFI 33-115, Volume 1, *Network Management*, 24 May 2006

AFI 33-118, *Electromagnetic Spectrum Management*, 18 July 2005

AFMAN 33-120, *Electromagnetic Spectrum Management*, 19 September 2006

AFI 33-129, *Web Management And Internet Use*, 3 February 2005

AFI 33-134, *Mobile Satellite Services Management*, 10 February 2005

AFI 33-200, *Information Assurance (IA) Management*, 23 December 2008, through Change 2, 15 October 2010

AFI 33-201, Volume 1, (FOUO) *Communications Security*, 1 May 2005

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, 1 May 2006

AFI 33-322, *Records Management Program*, 7 October 2003

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*, 1 June 2000

AFI 33-329, *Base and Unit Personnel Locators*, 23 August 2006

AFI 33-332, *Air Force Privacy Act Program*, 29 January 2004

AFI 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities*, Section 508, 9 January 2007

AFMAN 33-363, *Management of Records*, 1 March 2008AFI 90-301, *Inspector General Complaints*, 8 February 2005

AFSSI 8520, *Identification and Authentication*, 18 June 2009

AFRIMS RDS, <https://www.my.af.mil/gcss-af61a/afirms/afirms/>

AFOSH Std 48-9, *Radio Frequency Radiation (RFR) Safety Program*, 1 August 1997

MPTO 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements*, 14 April 2011

MPTO 00-33D-3003, *Methods and Procedures Managing the Cyberspace Infrastructure with the Cyberspace Infrastructure Planning System*, 30 December 2010

Prescribed Forms

No forms are prescribed by this publication.

Adopted Forms

AF Form 673, *Air Force Publication/Form Action Request*

AF Form 847, *Recommendation for Change of Publication*

DD Form 1435, *COMSEC Maintenance Training and Experience Record*

Abbreviations and Acronyms

24/7—All day/everyday

ADO—Activity Distribution Office

AF—Air Force

AFB—Air Force Base

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFNETOPS—Air Force Network Operations

AFNIC—Air Force Network Integration Center

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFSPC—Air Force Space Command

AIM—Asset Inventory Management

ANG—Air National Guard

ARM—Agency Records Manager
CAC—Common Access Card
C-E—Communications Electronics
CEG—Cyberspace Engineering Group
CIPS—Cyberspace Infrastructure Planning System
CIO—Chief Information Officer
COMPUSEC—Computer Security
COMSEC—Communications Security
COR—Chief of Office of Records
CRM—Command Records Manager
CRO—COMSEC Responsibility Officer
CSIR—Communications and Information Systems Installation Record
CSO—Communications and Information Systems Officer
DAA—Designated Accrediting Authority
DFAR—Defense Federal Acquisition Regulation
DoD—Department of Defense
DoDI—Department of Defense Instruction
DoDD—Department of Defense Directive
DoDM—Department of Defense Manual
DRU—Direct Reporting Unit
DSN—Defense Switched Network
EC—Equipment Custodian.
E&IT—Electronic and Information Technology
EIE—Enterprise Information Environment
EMSEC—Emission Security
ESI—Enterprise Software Initiative
EO—Executive Order
FAM—Functional Area Manager
FARM—Functional Area Records Manager
FOA—Field Operating Agency
FOIA—Freedom Of Information Act
GIG—Global Information Grid

GSU—Geographically Separated Unit
IA—Information Assurance
IAO—Information Assurance Officer
ICR—Information Collections and Reports
I-NOSC—Integrated Network Operations and Security Center
IM—Information Management
IRM—Information Resource Management
ISM—Installation Spectrum Manager
IT—Information Technology
I-TRM—Infrastructure - Technology Reference Model
ISSO—Information System Security Officer
JP—Joint Publication
KOM—Knowledge Operations Management
LRA—Local Registration Authority
MAJCOM—Major Command
MECO—MAJCOM Equipment Control Officer
MMSC—MAJCOM Message Service Centers
MPS—Military Postal Service
MPTO—Methods and Procedures Technical Order
MSS—Mobile Satellite Services
NCC—Network Control Center
NIPRNET—Non-Secure IP Router Network
NSS—National Security System
OSD—Office of the Secretary of Defense
PA—Privacy Act
PKI—Public Key Infrastructure
POC—Point of Contact
PPS—Ports, Protocols, and Services
RDS—Records Disposition Schedule
RF—Radio Frequency
RM—Records Manager
SAF—Secretary of the Air Force (organization)

SAP—Systems Applications and Products

SCI—Sensitive Compartmented Information

SECAF—Secretary of the Air Force (individual)

SIPRNET—Secure IP Router Network

SPO—Systems Program Office

STEM—Systems Telecommunications Engineering Manager

STEM—B-STEM-Base Level

STEM—C-STEM-Command Level

STEM—D-STEM-Deployability

STEM—E-STEM-Engineering

STEM—J-STEM-Joint

Terms

Accountable Officer—An individual appointed by proper authority who maintains item records and/or financial records in connection with Government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or for care and safekeeping.

Air Force Functional Manager—The HQ USAF activity within a specific directorate responsible for providing management oversight of the assigned function and its associated communications and information systems.

Automated Information System (AIS)—A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information.

Communications and Information System—An integrated combination of doctrine, procedures, organizational structures, personnel, equipment, C-E equipment and systems, facilities, and communications designed to support a commander's exercise of command and control through all operational phases. It includes base visual information support systems.

Communications and Information Systems Blueprint—Document in CIPS that provides the requirements engineering plan to modernize the installation level infrastructure with cost-effective, installation-wide capability to support digital transmission of voice, data, video, imagery, and telemetry needs. It documents the baseline, identifies a target base configuration to support present and future requirements, and provides a time-phased plan and estimated costs for logical transition.

Communications and Information Systems Officer (CSO)—The designated official who has overall responsibility for communications and information support at any given level of the Air Force (base, tenant, MAJCOM, USAF, etc.). At base level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of communications and information systems budgeted and

funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" and expands it to three and four letters to identify specific functional areas. CSOs are the accountable officer for all automated data processing equipment in their inventory.

Comprehensive Plan—The combination of the general plan, component plans, special plans and studies, and maps that document a wide range of information necessary for decision making. It encompasses those specific resource documents and processes determined to be essential for planning and managing an installation's physical assets in support of the mission. The comprehensive plan is the all-encompassing description of the products, whereas comprehensive planning is the action associated with the process and implementation.

Comprehensive Planning—The ongoing civil engineering process--iterative, participatory process addressing the full range of issues affecting or affected by an installation's development. Through this process, goals and objectives are defined, issues are identified, information is gathered, alternative solutions are developed, and a sound decision-making process is employed to select a preferred alternative for implementation. It incorporates Air Force programs such as operational, environmental, urban planning, and others, to identify and assess development alternatives and ensure compliance with applicable federal, state, and local laws; regulations; and policies.

Configuration Management—1. In computer modeling and simulation, a discipline of applying technical and administrative oversight and control to identify and document the functional requirements and capabilities of a model or simulation and its supporting databases, control changes to those capabilities, and document and report the changes. (Joint Publication [JP] 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994) 2. A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a C4 system; (b) to control changes of those characteristics; and (c) record and report changes to processing and implementation status.

Cyberspace—A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08)

Cyberspace Infrastructure—Physical structures required for cyberspace operations.

Cyberspace Infrastructure Planning System (CIPS)—Is the approved automated information system for planning, installing, and managing the Air Force's cyberspace infrastructure. It is a web-enabled certified and secure enterprise government system. It was developed to meet Congressional, Department of Defense, and AF policy. It is a key enabler of network centric operations (NWO) and is a critical tool in support of the AF Global Information Grid (GIG) and AF Network Operations (AFNETOPS). CIPS allows collaboration in documenting and tracking the installation of Information Technology on Air Force Installations.

Enterprise Information Environment (EIE)—The common, integrated information computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, provide transport for, and/or assure local area networks, campus area networks, tactical operational and strategic networks, metropolitan area networks, and wide area networks. The EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD

enterprise hardware, software operating systems, and hardware/software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. (DODD 8115.1, *Information Technology Portfolio Management*)

Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (see references). The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. (AFPD 33-4, *Enterprise Architecting*).

Information Resource Management (IRM)—The process of managing information resources to accomplish agency missions and to improve agency performance. This includes reduction of information collection burdens on the public. (AFPD 33-1, *Information Resource Management*)

Information System—A discrete set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (AFPD 33-1, *Information Resource Management*)

Information Technology—Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes equipment used by the executive agency directly or used by a contractor under a contract with the executive agency that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computer, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Notwithstanding the preceding, the term "IT does not include any equipment that is required by a federal contractor incident to a federal contract. The term IT includes National Security Systems (NSS), and is synonymous with the term "information system" (IS). (AFPD 33-1, *Information Resource Management*)

Interoperability—1. The ability to operate in synergy in the execution of assigned tasks. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*)

Knowledge Operations Management—Encompasses communications and data, information and knowledge management tasks and functions. Included are planning, coordinating,

managing, sharing, and controlling organization's data assets; conducting information analyses to determine proper flow and life-cycle management of information, regardless of medium; operating information systems to create, collect, process, disseminate, use, store, protect, and dispose of information; electronic and manual publications, and forms development, design, control, storage, and dissemination; management of official records, including manual and automated record management systems and operation of records staging, publishing and managing content through automated publishing tools; managing Privacy Act (PA) and Freedom of Information Act (FOIA) procedures; operating of Base Information Transfer System and Official Mail Center; serving as consultant/liaison for overall data, information, and knowledge planning and integration; using and managing technologies to capture, organize, and store activities/experiences; and client support administration, including management of computer hardware and software; installation and configuration of software operating systems and office automation applications, and configuration, management and initial diagnostics of information systems.

Lead Command—The MAJCOM or FOA assigned as systems advocate and oversight authority for communications and information systems used by more than one command. Specific responsibilities of the lead command are in AFI 10-901, *Lead Operating Command—Communications and Information Systems Management*.

Modification—A temporary or permanent change to a system that is still being produced. The purpose of the modification is to correct deficiencies, improve reliability and maintainability, or to improve capabilities.

National Security System (NSS)—Any telecommunications or information system (IS) operated by the U.S. Government, the function, operation, or use of which: 1) involves intelligence activities; 2) involves cryptologic activities related to national security; 3) involves command and control of military forces; 4) involves equipment that is an integral part of a weapon or weapons system; or 5) is critical to the direct fulfillment of military or intelligence missions (this does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications). (AFPD 33-1, *Information Resources Management* (**Note:** For information assurance (IA) purposes only pursuant to AFPD 33-2, *Information Assurance (IA) Program*), the term NSS also includes any telecommunications or IS that is protected at all times by procedures established for managing classified information.

Nonmaterial Solution—Includes changes in doctrine, operational concepts, tactics, training, or organization.

Responsible Officer—An individual appointed by proper authority to exercise custody, care, and safekeeping over property entrusted to his or her possession or under his or her supervision.

Systems Telecommunications Engineering Manager (STEM)—A communications and information systems engineer who provides technical engineering planning services in support of facilities and base infrastructures. The STEM-B has technical responsibility for engineering management and assists the base CSO in system engineering and configuration control. The STEM-C provides technical assistance to the MAJCOM and coordinates with STEM-Bs on future MAJCOM mission changes, programs, and efforts at the MAJCOM-level. The STEM-J is assigned to combatant commands (COCOM), and AF Forces (AFFORs) to promote interoperability by providing an interface between those activities and the Air Force MAJCOMs

and bases. The STEM-D supports the COCOMs providing master planning services in support of command, control, communications and computer (C4) systems to complement the base comprehensive plans or future development plans at bases in deployed locations. STEM-PMs are Program/Project Managers who are responsible for facilitation, oversight, and coordination of all programs/projects that have been funded and are assigned to the 38 CEG for implementation.

Attachment 1 (ELLSWORTHAFB)**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 33-101, *Commanders Guidance and Responsibilities*, 18 Nov 2008, Incorporating Change 1, 21 Jul 2011

AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation (MWR) and Non-appropriated Fund Instrumentalities (NAFIS)*, 6 May 2009

AFPD 33-1, *Cyberspace Support*, 9 Aug 2012

AFMAN 23-110, *United States Air Force Supply Manual*, 1 Apr 2009, Incorporating through Interim Change 10, 1 Oct 2011

AFMAN 33-363, *Management of Records*, 1 Mar 2008

Adopted Forms

Form 847, *Recommendation for Change of Publication*

Acronyms and Abbreviations

28 BW/PA—28th Bomb Wing Public Affairs

28 CS—28th Communications Squadron

28 CS/SCO—28th Communications Squadron Flight Commander, Operations Flight

28 CS/SCOS—28th Communications Squadron Client Systems Center

ABU—Airman Battle Uniform

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

EAFB—Ellsworth Air Force Base

OPR—Office of Primary Responsibility

PA—Public Address

PAC—Public Address Coordinator

POC—Point of Contact

PBSA—Performance-Based Services Acquisition

WOMS—Work Order Management System

Attachment 2**COMMUNICATIONS AND INFORMATION SYSTEMS OFFICER DUTIES****A2.1. MAJCOM CSO and information staff element will:**

A2.1.1. In conjunction with the command-level systems telecommunications engineering manager (STEM-C), develop the MAJCOM Blueprint in CIPS identifying the target architecture to meet specific MAJCOM mission capabilities taking into consideration AF Cyberspace objectives. Be responsible for narrative information on the MAJCOM Blueprint Executive Summary (capabilities based planning) and Transition Strategy. Reference MPTO 00-33D-3003 for CIPS procedures.

A2.1.2. Use configuration management methods to ensure the integrity and interoperability of systems.

A2.1.3. Plan, program, and budget for engineering, installation, operation, and maintenance of MAJCOM-unique systems and the command's portion of Air Force-wide systems.

A2.1.4. Work with the STEM-C and STEM-J (AFFOR requirements) to prioritize command-wide requirements for inclusion into Air Force/MAJCOM work plan(s) that is/are ready for execution. Be the "Approval" authority of all MAJCOM work plans in CIPS which correlate into current year spend plans.

A2.1.5. Be the "Acceptor" of the Wing Approved Base Blueprints, ensuring architectural compliance, proper classification, and functional support. Be responsible for narrative information on the MAJCOM Blueprint Executive Summary (capabilities based planning) and transition strategy. Ensure that the blueprints within CIPS incorporate the civil engineers base comprehensive plans and military construction programs to identify funding for MILCON projects and resolve conflicts between long-range C4ISR plans and the base comprehensive plan.

A2.1.6. Develop a process to review MAJCOM C&I requirements.

A2.1.7. Provide guidance and procedures to identify and communicate special engineering, installation, operations and/or maintenance requirements for NSS, Systems Applications and Products (SAP) or Sensitive Compartmented Information (SCI) or other federal agency systems utilized by their units to appropriate AF authorities (i.e. AFNETOPS/CC, Air Staff, I-NOSCs, etc.).

A2.2. Installation CSO will:

A2.2.1. Organize, train, and lead all units assigned communications and information personnel.

A2.2.2. Meet wing's communications and information mission needs to include planning, organizing, and deploying communications and information systems to support the wing or its elements when they deploy.

A2.2.3. Ensure elements of the installation communications and information environment and infrastructure, including mobile assets, continue to satisfy customers' mission needs.

A2.2.4. Manage the installation level infrastructure, host systems, and tenant systems as defined in support agreements, and establish an installation systems integration function.

A2.2.4.1. Serve as the focal point for the installation's non-mission systems needs and as the accountable officer for all IT hardware equipment accounted for in their assigned Asset Inventory Management (AIM) Defense Reporting Activity (DRA).

A2.2.4.2. Appoint an Equipment Control Officer to oversee the installation AIM program IAW AFI 33-112, *Information Technology Hardware Asset Management*.

A2.2.5. Plan the evolution of systems supporting the installation users' missions; ensure war, support, and contingency planning are accomplished for communications and information requirements.

A2.2.6. Develop communications and information annexes and appendices, contingency plans and support plans. Review and assist with the development of tenant plans involving communications and information resources or activities.

A2.2.7. Identify and collect cyberspace infrastructure requirements and incorporate them into the CIPS base blueprint, as necessary. Work with the STEM-B to integrate base requirements into prioritized project plans that can be submitted to an appropriate Air Force/MAJCOM work plan. Reference MPTO 00-33D-3003.

A2.2.8. Coordinate with the 38th Cyberspace Engineering Group (CEG) assigned base-level STEM (STEM-B) on the blueprint endorsement.

A2.2.9. Coordinate STEM-B visits with installation level Functional Area Managers (FAMs).

A2.2.10. Coordinate the communications and information systems blueprint with the host wing and other tenant units. Ensure the communications and information systems blueprint in CIPS, the installation comprehensive plan, and military construction programs complement each other (see AFI 32-7062, *Air Force Comprehensive Planning*).

A2.2.11. If the wing commander delegates, serve as base-level approval authority for the Implementation Document and other requirements documents submitted for implementation of communications and information systems.

A2.2.12. Serve as the overall interface with the STEM-B to establish priorities and render decisions concerning the base communications and information infrastructure.

A2.2.13. Manage communications and information projects.

A2.2.13.1. Manage all Communications and Information Systems Installation Records (CSIR) for inside plant per MPTO 00-33A-1001 in CIPS.

A2.2.13.2. Manage the outside plant Communications Mission Data Set (CMDS) layer in the CIPS Visualization Component (CVC) per MPTO 00-33D-3003.

A2.2.14. DELETED.

A2.2.15. Appoint in writing a primary and alternate base inside plant CSIR manager.

A2.2.15.1. DELETED.

A2.2.16. Prevent or minimize electromagnetic interference and electromagnetic radiation hazards (see AFOSH STD 48-9, *Radio Frequency Radiation (RFR) Safety* and AFI 10-707, *Spectrum Interference Resolution Program*).

A2.2.17. Manage the installation frequency management program and follow the AF Spectrum Interference Resolution Program reporting procedures and guidance in AFI 10-707, *Spectrum Interference Resolution Program* (see paragraph 4.2).

A2.2.17.1. The CSO will appoint, a primary and alternate Installation Spectrum Manager (ISM) to organize and carry out the spectrum management program in accordance with AFI 33-118, *Electromagnetic Spectrum Management* and AFMAN 33-120, *Electromagnetic Spectrum Management* and forward appointment letter to Air Force Frequency Management Agency (AFFMA).

A2.2.18. Establish a focal point for determining installation level communications and information training and provide for customer support.

A2.2.19. Account for all IT assets according to AFI 33-112, *Information Technology Hardware Asset Management* (see paragraphs 4.3 and 4.4).

A2.2.19.1.1. Asset Inventory Management (AIM) is the AF official accountable property system of record for IT hardware assets.

A2.2.20. Establish a single customer contact for automated systems and network problems, system administration requirements, and system and network protection requirements (such as an AF Network Control Center) (see AFI 33-115, Volume 1, *Network Operations (NETOPS)*).

A2.2.21. For installations with deployable wings, provide trained personnel and sufficient equipment to support the wing's deployable commitments.

A2.2.22. Establish a periodic wing-level planning forum to discuss current and future issues affecting the wing's communications and information infrastructure and the various systems it supports. Involve the STEM-B in the wing-level planning forum.

A2.2.23. Assign an individual as the Wing/Base Knowledge Operations Management (KOM) Functional Manager for accession, training, classification, utilization, and career development of enlisted KOM (AFSC 3D0X1) personnel. These personnel operate in every functional area and, although most are not assigned to the communications unit, they are specialized extensions of the total capability for A6 to support the AF mission. A network of open communications is critical among these personnel at all levels.

A2.2.24. Provide training to all unit Telephone Control Officers (TCO) upon initial appointment by a unit commander or equivalent on TCO duties and responsibilities. Brief all TCOs at least annually on policy changes and their duties and responsibilities.

A2.3. Tenant Unit CSO will:

A2.3.1. Serve as their single focal point and accountable officer for communications and information systems of their respective activities. Define specific tenant and base CSO responsibilities in a support agreement or similar document.

A2.3.2. Coordinate with the installation CSO to ensure their systems will integrate and interoperate, when necessary, with the Defense information infrastructure, and Air Force and host base systems.

A2.3.3. Identify to the host installation, MAJCOM and AFNetOps special engineering, installation, operation and/or maintenance requirements for NSS, SAP or SCI or other federal agency systems that are used by the tenant.

Attachment 3

DELETED

Attachment 4 (Added-ELLSWORTHAFB)**PUBLIC ADDRESS (PA) RESPONSIBILITIES AND PROCEDURES****A4.1. (ELLSWORTHAFB) Definitions:**

A4.1.1. **(ELLSWORTHAFB) Fixed Public Address (PA) System.** A system permanently installed in a base facility.

A4.1.2. **(ELLSWORTHAFB) Portable PA System.** A system set-up on a temporary non-repetitive basis for any function of short duration.

A4.1.3. **(ELLSWORTHAFB) Portable PA System for Sign Out.** A system signed out by the requesting office, set-up on a temporary, non-repetitive basis for any function of short duration.

A4.1.4. **(ELLSWORTHAFB) Routine PA Request.** Any request for PA support with 10 or more duty day's notice.

A4.1.5. **(ELLSWORTHAFB) Short-Notice PA Request.** Any request for PA support with 4 – 9 duty days' notice.

A4.1.6. **(ELLSWORTHAFB) Emergency PA Request.** Any request for PA support with less than 72 hours notice.

A4.1.7. **(ELLSWORTHAFB) Official Function.** A direct military related function such as a change of command, retreat, retirement ceremony, dining-in, commander's call, etc. PA requests for functions supporting base community relations, such as heritage associations, Boy Scouts, Special Olympics, or other special events must be approved by 28th Bomb Wing Public Affairs (28 BW/PA) office to be deemed official prior to submission.

A4.1.8. **(ELLSWORTHAFB) Unofficial Function.** A function whose primary intent is to entertain. Portable PA support for events such as unit parties, picnics, sporting events is considered unofficial and can only be supported if authorized by the 28 CS Flight Commander, Operations Flight (28 CS/SCO) in writing.

A4.1.9. **(ELLSWORTHAFB) Public Address Coordinator (PAC).** The 28 CS Client Systems Center (28 CS/SCOS) technician assigned to your PA event. This person is the Customers' Point of Contact (POC) from the 28 CS/SCOS.

A4.2. (ELLSWORTHAFB) Responsibilities:

A4.2.1. **(ELLSWORTHAFB)** The primary mission of 28 CS/SCOS is to direct, control and report all communications maintenance. The 28 CS/SCOS serves as the squadron's operational command and control support element, ensuring timeliness and effectiveness of maintenance activities and status reporting. Any outage affecting, or potentially affecting the base mission has priority over PA support.

A4.2.2. **(ELLSWORTHAFB)** The Customer:

A4.2.2.1. **(ELLSWORTHAFB)** Responsible for submitting, Public Address Support Request online form located on the Air Force (AF) Portal under "Operations Flight (SCO)" as "Public Address Support Request", at least ten days prior to event.

A4.2.2.2. **(ELLSWORTHAFB)** Responsible for reserving the facility where a fixed or portable system will be used, (i.e. base theater, Dakota Club, and so forth).

A4.2.2.3. **(ELLSWORTHAFB)** Provide a meal at no cost to the operator of PA system when supported function includes a meal for guests.

A4.2.2.4. **(ELLSWORTHAFB)** Coordinate the use of fixed PA systems through the appropriate responsible agency.

A4.2.2.5. **(ELLSWORTHAFB)** Provide podiums for use during the event. **NOTE:** The base theater and the Dakota Club each have a podium available for use in these facilities.

A4.2.2.6. **(ELLSWORTHAFB)** Building custodians are responsible for providing fixed PA equipment in facilities used by base personnel. Base Contracting will assist units requiring fixed/portable PA systems with contract support for installation and maintenance in accordance with AFI 63-124 Performance-Based Services Acquisition (PBSA). 28 CS/SCOS maintains/operates 28 CS equipment installed in the base theater and the Dakota Club. (Refer to paragraph A4.3.1, this instruction, for further guidance).

A4.2.3. (ELLSWORTHAFB) The 28 CS:

A4.2.3.1. **(ELLSWORTHAFB)** Provide portable PA equipment to support official functions and approved unofficial functions.

A4.2.3.1.1. **(ELLSWORTHAFB)** Set-up PA equipment for retirement ceremonies for pay grades 0-5 or equivalent rank or civilian pay grade and above, E-7 or equivalent rank or civilian pay grade and above, or hosted by Group Commander or above. For other retirement ceremonies, portable PA systems can be signed out (see paragraph A4.3.3, this instruction).

A4.2.3.1.2. **(ELLSWORTHAFB)** Provide portable sign out equipment for commander's calls and change of command events at squadron/unit level organizations on a first come, first served basis. Permanently installed systems at the base theater and Dakota Club are available to routinely support these types of functions.

A4.2.3.1.3. **(ELLSWORTHAFB)** Under no circumstances will a PA system be provided for any profit making events in accordance with AFI 65-106.

A4.2.3.2. **(ELLSWORTHAFB)** All PA requests will be assigned a PAC by 28 CS/SCOS.

A4.2.3.2.1. **(ELLSWORTHAFB)** Responsibilities of the PAC.

A4.2.3.2.1.1. **(ELLSWORTHAFB)** Verifying customer requirements are understood and will contact the customer for clarification as necessary.

A4.2.3.2.1.2. **(ELLSWORTHAFB)** Ensure all proper equipment is on site.

A4.2.3.2.1.3. **(ELLSWORTHAFB)** Perform a complete sound check of all sound equipment during set-up with customer to ensure set-up is satisfactory.

A4.2.3.2.1.4. **(ELLSWORTHAFB)** Duty Uniform for Public Address Support. During normal duty hours, personnel providing PA support will wear airman

battle uniform (ABU) or unobtrusive attire commensurate with the function. After normal duty hours, (Dining In/Out, award ceremonies, banquets, etc.) the point of contact must annotate the uniform of the evening on the request form. When the function requires formal/semi-formal dress, the PA technicians will wear blues (long- or short-sleeved shirt with tie/tab). When the function requires civilian attire, the PA technicians will wear presentable civilian attire (no blue jeans, T-shirts, or offensive clothing). The PA technician in charge of the setup will ensure all technicians are wearing the proper uniform.

A4.2.3.3. **(ELLSWORTHAFB)** 28 CS/SCOS personnel will not be tasked to operate fixed PA systems belonging to another unit unless approved by the 28 CS/SCO.

A4.2.4. **(ELLSWORTHAFB)** The 28 CS/SCO is the approval authority for all requests for portable PA set-ups to be accomplished by the 28 CS/SCOS work center, except those specifically authorized by paragraph A4.1.7. of this instruction. The 28 CS/SCO determines the level of support given when there is a conflict between two different PA set-ups at the same time.

A4.2.5. **(ELLSWORTHAFB)** 28 CS/SCOS, 28 CS/SCO, or 28 CS/CC may cancel PA set-ups or remove PA equipment from operation if personnel or equipment safety is threatened (that is, during inclement weather).

A4.2.6. **(ELLSWORTHAFB)** Disc jockey services for any PA set-up will not be provided.

A4.3. (ELLSWORTHAFB) Procedures:

A4.3.1. **(ELLSWORTHAFB)** Requesting PA equipment set-up by 28 CS:

A4.3.1.1. **(ELLSWORTHAFB)** Call 28 CS/SCOS at 385-2666 for guidance in requesting PA support. Support requests must be submitted to 28 CS/SCOS using the online form located at the AF Portal under "Operations Flight (SCO)" as "Public Address Support Request", not less than 10 duty days prior to the day of the event. This is to provide adequate time for processing and scheduling, and also provide the requesting unit time to locate an alternate source in the event a request is denied or cannot be satisfied. Forms are filed in the 28 CS/SCOS work center. They are destroyed after the 3 month cutoff or when no longer needed, whichever is sooner.

A4.3.1.2. **(ELLSWORTHAFB)** The following procedures will be followed when requesting PA systems support.

A4.3.1.2.1. **(ELLSWORTHAFB)** Portable PA request for location outside the perimeter of EAFB must be requested, in writing, to 28 BW/PA office and approved by 28 CS/SCO.

A4.3.1.2.2. **(ELLSWORTHAFB)** The requesting unit POC is required to contact 28 CS/SCOS if changes occur and encouraged to contact us with questions or concerns at 385-2666.

A4.3.1.2.3. **(ELLSWORTHAFB)** 28 CS/SCOS personnel will normally accompany equipment they set-up to ensure continuous operation unless precluded by higher priority mission requirements or lack of manpower. If a 28 CS/SCOS technician cannot stay or is not required to stay with the system, the PA system users will be required to sign an AF Form 1297, *Temporary Issue Receipt*, for the equipment.

Organizations requesting PA equipment music support (cassette, CD) will provide a person to start and stop music at the appropriate times.

A4.3.1.2.4. **(ELLSWORTHAFB)** Official functions will be supported by the full complement of PA equipment at the final ceremony only. Sound requirements for practices must be scheduled in advance. Customers may sign out a portable PA system for practices, if available.

A4.3.1.2.5. **(ELLSWORTHAFB)** All agencies (that is, base visual information, public affairs, local media, and so forth) requesting interface with the 28 CS PA system will be connected and tested not less than 1 hour prior to the start of an event. 28 CS/SCOS needs to be notified for any planned interface not less than 2 days in advance. Should this additional equipment cause interference with the PA system, the 28 CS/SCOS technician is authorized to disconnect equipment and deny the interface.

A4.3.2. **(ELLSWORTHAFB)** Obtaining Portable PA Systems for Sign Out to the Office of Primary Responsibility (OPR) for Official Functions and Approved Unofficial Functions:

A4.3.2.1. **(ELLSWORTHAFB)** 28 CS/SCOS has portable systems for sign-out. Call 385-2666 for availability and/or suggestions on portable systems. Training is provided at the time of receipt to ensure the OPR can operate the equipment. PA equipment signed out can be picked up at building 7235 room 11, 1 duty day prior to the event and must be returned no later than 0800 the first duty day after the event.

A4.3.2.2. **(ELLSWORTHAFB)** All PA equipment is signed out on an AF Form 1297 at the time it is borrowed. Equipment must be returned in good condition. Coil and tape or tie cables to prevent tangling prior to turn in. Identify broken parts, problems, or discrepancies when the equipment is returned. The OPR is responsible for any lost or damaged equipment.

A4.3.3. **(ELLSWORTHAFB)** The 28 CS/SCOS is not responsible for procurement, installation or maintenance of PA systems for other base units. Fixed PA systems can be obtained as outlined in AFI 33-103. Installation and maintenance should be obtained through the Base Contracting Office. Permanently installed PA systems are justified and procured by the using organization in accordance with Table of Allowance 006 and AFMAN 23-110. 28 CS/SCOS may be used as a technical consultant on PA system acquisition by properly submitting a Work Order Management System (WOMS) request through the Plans and Programs Flight 28 CS/SCX.